State redistribution as merging: introducing the coherent relay

Jonathan Oppenheim[1]

[1]*Department of Applied Mathematics and Theoretical Physics, University of Cambridge U.K.*

State redistribution allows one party to optimally send part of her state to another party. Here we show that this can be derived simply from two applications of coherent state-merging. This provides a protocol whereby a middle party acts as a relay station to help another party more efficiently transfer quantum states. This also gives a protocol for state splitting and the reverse Shannon theorem (assisted or unassisted by side information), and allows one to use less classical communication for partial state-merging using a sub-protocol we call *ebit repackaging*. Thus state-merging generates the other primitives of quantum communication theory, reducing the hierarchy between members of the first family of quantum protocols.

In [1, 2] the problem of state redistribution was considered. Namely, Alice and Bob share a quantum state, and Alice wants to send part of her state to Bob by sending only quantum states and using pre-shared entanglement. In such a situation Alice can use the part of the state she doesn't send to Bob in order to send less than if she didn't have access to this part. The proof of this, and the resulting protocol were fairly complicated [2]. Here, we show a simple and transparent protocol for state redistribution using state-merging [3, 4]. This leads to another way to organise the family of protocols [5] which form the basic building blocks of quantum communication theory. It also provides a new protocol for several other common tasks including a version of quantum state merging using less classical communication in the case that part of the state remains at the sender's site.

In state redistribution, Alice and Bob share n copies of state ρ_{ABC} with Alice holding onto $\rho_{AC} = \mathrm{Tr}_B\, \rho_{ABC}$. One imagines a total pure state $|\psi\rangle_{ABCR}$ by introducing a reference system R. The task is for Alice to transfer ρ_A to Bob while otherwise keeping the overall state $|\psi\rangle_{ABCR}^{\otimes n}$ virtually unchanged (in terms of fidelity). The protocol is allowed to consume (or produce) ebits i.e. shared entanglement in state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

If all that is available to Alice and Bob is a quantum channel, then Alice can send her share A to Bob using $nI(A : R|B)/2$ qubits [1] where the mutual information is defined as $I(C : R) = S(C) + S(R) - S(CR)$ and $I(A : R|B) = S(A|B) + S(R|B) - S(AR|B)$ with $S(A|B)$ the conditional entropy defined as $S(AB) - S(B)$. The optimal protocol also consumes ebits at a rate of $E = I(A : C)/2 - I(A : B)/2$. If this quantity is negative, that this amount of entanglement is produced.

We will show that redistribution uses *quantum state merging* as a basic primitive. In state merging Alice and Bob share n copies of state ρ_{AB}, and Alice is able to optimally transfer her state to Bob using $nS(A|B)$ ebits and $nI(A : R)$ bits of classical communication (the result x of a random measurement she performed on her state).

Now, to perform merging with a quantum channel instead of a classical one, the sender is forced to send the classical measurement result x using the quantum channel. This gives a coherent version of merging, sometimes called the Fully Quantum Slepian Wolf Theorem (FQSW) or *merging mother* [5, 6]. One can derive this coherent-merging from the original merging protocol by sending the classical communication using super-dense coding [7]. This consumes $nI(A : R)/2$ ebits, and requires that $nI(A : R)/2$ qubits be sent. However, Alice could also make the measurement coherently i.e. perform a cnot operation from her state to an ancilla prepared in the $|0\rangle$ state and store the measurement result x as the state $|x\rangle|x\rangle$. One half of this state can then be encoded and sent using super-dense coding. Since the measurement result x is independent of the final state after the protocol and is distributed uniformly, this generates $nI(A : R)/2$ ebits (i.e. $\sum_x |x\rangle|x\rangle$). Adding these generated ebits to the initial $nS(A|B)$, yields a total gain of $nI(A : B)/2$ ebits and a cost of $I(A : R)/2$ sent qubits.

A direct protocol for achieving this rate[5] is for Alice to apply a random unitary U to her state and an ancilla of $nI(A : R)/2$ qubits initialised to $|0\rangle$, and then send this ancilla to Bob. Bob then performs a decoding unitary V on his system and the sent qubits. As a result, Bob will possess ρ_{AB} and the two parties share $I(A : B)/2$ ebits.

A naive application of coherent-merging in the case when Alice also holds share ρ_C would require n$I(A : RC)/2$ qubits to transfer ρ_A to Bob since ρ_C would be treated as the reference system to which correlations have to be maintained. However, if Alice makes use of ρ_C then redistribution only requires $nI(A : R|B)/2$ qubits, a saving of $nI(A : C)/2$ qubits.

We now show that a less naive application of coherent-merging can be used as a primitive to perform state redistribution. The essence of the idea is that Alice should not attempt to send all of ρ_A to Bob, and in particular should not send the pure state entanglement which exists between A and C. This pure state entanglement can instead be extracted at a rate of $I(A : C)/2$, and replaced by ebits which were pre-shared between Alice and Bob, thus reducing the number of qubits which have to be sent. One shouldn't waste the quantum channel to transfer ebits.

For the purpose of the protocol we will imagine that

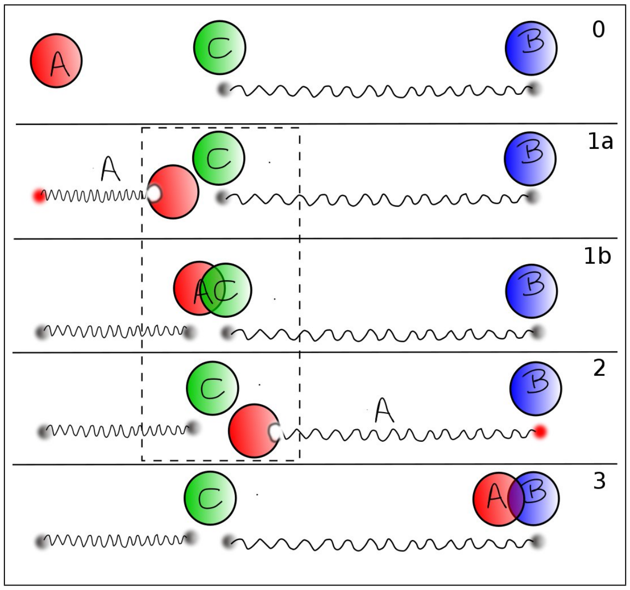

FIG. 1: The protocol. Shares of state ρ_{ABC} are represented by circles, while shared entanglement is represented by wiggly lines. The key difference between the situation depicted in $1a$ and 2 is that $I(A:C)/2$ qubits (highlighted in red) have in effect been transferred from Alice to Bob. The steps refer to those in the protocol below and the sub-protocol of repackaging is contained in the dashed square.

Alice is split into two parties, one holds ρ_A (we will give this party the name Alice) and Charlie who holds ρ_C. As a result, we will actually get a more general three party protocol with Charlie acting as a relay station, minimising the number of qubits sent to Bob.

Protocol: redistribution from merging

1: Alice coherently merges ρ_A to Charlie. This extracts a rate of $I(A:C)/2$ ebits, and uses the quantum channel between Alice and Charlie at a rate of $I(A:RB)/2$. We can break this into two steps. **1a:** Alice applies the random unitary U and sends to Charlie $nI(A:RB)/2$ qubits. **1b:** Charlie applies the decoding unitary V on his state and the qubits from Alice, generating $I(A:C)/2$ ebits between himself and Alice

2: Charlie sets aside the ebits that were generated from the previous step and replaces them with ones shared between him and Bob. He then applies $V^\dagger$.

3: The effect of the previous step is no different from Alice having transferred $nI(A:C)/2$ qubits to Bob. Charlie then sends the remaining $nI(A:CR)/2 - nI(A:C)/2$ qubits needed to transfer ρ_A to Bob. This leaves him with $nI(A:B)/2$ qubits which are in fact ebits between himself and Bob.

The key element is that the qubits that Alice sent to Charlie are no different to the ones she kept behind, except in the amount. Thus, after step 2, the situation is completely equivalent to Alice having sent $nI(A:C)/2$ qubits. Since a naive coherent-merging protocol requires $nI(A:RC)/2$ qubits to be sent from Alice to Bob, and the *ebit repackaging* performed in steps $1a-2$ are completely equivalent to Alice having already sent $nI(A:C)/2$ qubits to Bob, all that remains to be sent are $nI(A:R|B) = nI(A:RC)/2 - nI(A:C)/2$ qubits. Accounting for sent qubits $Q^{A\to C}$ between Alice and Charlie and $Q^{C\to B}$ between Charlie and Bob, as well as consumed ebits E_{AC} and E_{BC} we have the optimal rate pairs

$$Q^{A\to C} = \tfrac{1}{2}I(A:RB) \ \ , \ \ E^{AC} = \tfrac{1}{2}I(A:C)$$
$$Q^{C\to B} = \tfrac{1}{2}I(A:R|B) \ \ , \ \ E^{CB} = \tfrac{1}{2}I(A:C) - \tfrac{1}{2}I(A:B)$$

Interestingly, in the sub-protocol of ebit repackaging (steps $1a-2$), ρ_C is needed but is not changed, acting as a catalyst. Ebit repackaging can be used in other protocols. If one performs repackaging before applying the random measurement used in state merging (on what remains of ρ_A), then it reduces the amount of classical communication needed in the case when only ρ_A is merged – only $I(A:R|B)$ classical bits are used, rather than $I(A:RC)$. The case of redistribution when ρ_B is null is called state-splitting (or the Fully Quantum Reverse Shannon Theorem). The time reverse of state-redistribution is a coherent version of the reverse Shannon theorem aided by side-information at a relay station. Repackaging gives a protocol for these tasks as well.

It was previously believed that state redistribution was a more general primitive which could be used to construct the other building blocks of quantum communication theory, such as coherent-merging, which could then be used to construct the merging protocol and the so-called father protocol as well as many others. Here, we see that a number of primitives can generate the other building blocks of quantum Shannon theory – we have shown how merging can be used as a primitive to construct state redistribution and coherent-merging. Likewise, coherent-merging can generate redistribution and merging.

Acknowledgements. I thank Igor Devetak for interesting discussions. This work is supported by the Royal Society, and EU projects SCALA and QAP.

[1] I. Devetak and J. Yard (2006), quant-ph/0612050.
[2] J. Yard and I. Devetak (2007), quant-ph/07062907.
[3] M. Horodecki, J. Oppenheim, and A. Winter, Nature **436**, 673 (2005), quant-ph/0505062.
[4] M. Horodecki, J. Oppenheim, and A. Winter, Comm. Math. Phys. **269**, 107 (2006), quant-ph/0512247.
[5] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter (2006), quant-ph/0606225.
[6] I. Devetak (2005), quant-ph/0505138.
[7] C. Bennett and S. Wiesner, Phys. Rev. Lett **69**, 20 (1992).